UDC 376
DOI: 10.15587/1729-4061.2023.273973

DEVELOPMENT OF A CROPPING RESILIENT WATERMARKING SCHEME BASED ON CONTOURLET TRANSFORM FOR SECURE IOT COMMUNICATION

The objective of this work is to propose a robust watermarking method as watermarking techniques are widely used today for preventing image altering and duplication. With the growth of image-based IoT applications nowadays, the need for developing robust digital watermarking techniques is of high demand. In this work, a robust yet highly perceptible watermarking scheme is proposed. The proposed scheme is based on the Contourlet Transform (CT) and Singular Value Decomposition (SVD) as the embedding domain in which the high-frequency components are chosen for embedding. The frequency domain is selected in order to make the watermarking scheme resists image attacks as the watermark is spreaded across different frequency bands in the cover image and hence the possibility of altering all the embedded bands is not possible as it will results in destroying the cover image. On the other hand, the Arnold transformation was used to insure secure IOT communication where the Arnold transform is applied to the binary logo watermark before embedding for a more secure design. In this context, the host image has been decomposed into the first level of contourlet transform and the highest frequency sub-bands are selected for embedding after performing the SVD on those bands where the SVD matrix is chosen to be the embedding domain. Moreover, This work aims to resist the cropping attack on images where PSNR values were above 52 dB and NC values ranged from 0.8 to 0.9 under various types of cropping attacks. In addition, the proposed method demonstrates its ability to resist various geometric and noise attacks such as JPEG compression, histogram equalization, gaussian noising and image brightening. Comparisons with state-of-the-art work demonstrate the proposed scheme's efficiency

Keywords: contourlet transform, watermarking, Arnold transform, geometric attacks, cropping attack, SVD

Yahya Idham
Corresponding author
Master*
E-mail: yahya.idham@uoninevah.edu.iq
Omar Alsaydia
Master of Science in Computer Network, Assistant Lecturer*
Mohammed A. M. Abdullah
PhD*
Ahmed Mohammed
Lecturer, Master*
Ersin Elbasi
PhD
College of Engineering and Technology American University of the Middle East
Egaila, Kuwait, 54200
*Department of Computers and Information
College of Electronics Engineering
Ninevah University
Al Majmoaa str., Mosul, Iraq, 41001

Received date 16.11.2022
Accepted date 26.01.2023
Published date28.02.2023

***How to Cite**: Idham, Y., Alsaydia, O., Abdullah, M. A. M., Mohammed, A., Elbasi, E. (2023). Development of a cropping resilient watermarking scheme based on contourlet transform for secure iot communication. Eastern-European Journal of Enterprise Technologies, 1 (2 (121)), 21–28. doi: https://doi.org/10.15587/1729-4061.2023.273973*

1. Introduction

Secure transmission and privacy issues are a hot topic nowadays specially in IoT devices [1]. As a solution to illegal access to the IoT, devices must maintain high privacy protection, anonymization of data, and a strong authentication mechanism to protect information from illegal access [2]. Moreover, IoT device communications include digital image transmission and these images are impressionable to illegal modification and copying. Misinterpretation is possible if these malicious modifications are applied when the integrity of image verification is disabled [3] which may lead to altering the image information. For example, a medical image modification may result in a false diagnosis. Due to the aforementioned issues, digital images employed in IoT communications must be protected in terms of integrity and copyright protection. Such protection could be achieved easily through watermarking [4].

Generally speaking, digital watermarking is divided into two main stages, the embedding stage and the extractions stage. As for the first stage, the watermark/payload is embedded into the host image using various embedding algorithms depending on the scheme design and the purpose of protection. In the second stage, the watermark extraction is carried out and the extracted watermark must be compared against the original embedded payload for the sake of integrity verification [5]. In this context, watermarking can be performed using two main domains, namely: watermarking in the spatial domain and frequency domains [6]. The watermark is injected into the pixel values of the host image in the spatial domain by modifying the pixel values themselves. This method has the advantage of low computational cost. On the other hand, the main disadvantage is presented by the low robustness as losing random pixel values from the watermarked host image has a direct negative impact on the extraction process, especially when using a geometrical attack such as the cropping attack [7]. To enhance the robustness, the frequency domain is preferred where the embedding process is performed by inserting a watermark in different frequency bands and hence it has higher resistance against attacks such as JPEG compression attack, blur attack and sharpening attack. Among different frequency transforms, the most common ones are the Discrete wavelet transform (DWT), Discrete cosine transform (DCT), Discrete Fourier transform (DFT), and Singular value decomposition (SVD).

In the aforementioned attacks, a part of the watermarked image is cropped or trimmed which in turn results in a partial or full loss to the embedded watermark. This type of attack could be more threatening if 80 % or even 90 % of the image is cropped [8]. The situation is more challenging when more than one part of the watermarked image is being cropped which can be considered a dual attack. This type of attack has not been well addressed in state-of-the-art work.

Therefore, studies that are devoted developing robust watermarking scheme capable of tolerating large part of the watermarked image being cropped are scientific relevance.

2. Literature review and problem statement

Several works were proposed that employed watermarking for image integrity protection. In [9] the authors have proposed fast multiple zero watermarking algorithms in medical images using Multi-Channel Fractional Legendre Fourier moments (MFrLFMs) algorithm. The proposed algorithm provides high accuracy, robustness and resistance against common signal processing attacks in terms of physical layer watermarking. The researchers in [10] applied the discrete wavelet transformation algorithm to embed and retrieve secret information. In their work, the pseudo-random number is embedded as secret information. In the detection process, DWT based method gives very low error. In [11] authors applied redundant discrete wavelet transform (RDWT), Hessenberg Decomposition (HD), and randomized singular value decomposition (RSVD) algorithms to the COVID-19 CT images for patient data privacy. The proposed dual watermarking system gives very promising results in CT and other medical images. PSNR, NC, and SSIM metrics show very good results for medical MRI and CT images. It is also very strong against geometric attacks such as resizing, rotation, scaling, and cropping. However, the work [11], cannot tolerate the cropping attack when 80% of the image is removed. Authors of [12] proposed adaptable scaling factor-based watermarking to achieve more robust and secure embedding. In both DWT and DCT, most of the algorithms use scaling factors in the embedding formula. The usage of the best scaling factor increases robustness and produces high invisibility in the images. Instead of a single watermark, using a multi-watermark provides security against theft and changes in multimedia elements.

The paper [13] has proposed lifting wavelet watermarking, DCT, and ACM using multi-watermark. The cover image is transformed into two-level LWT, then low frequencies are transformed into the DCT. Multi watermark is embedded into the coefficients using the Arnold Cat map algorithm. Experimental results show very promising results after the embedding and binary multi-watermark extraction. NC values are very high in Gaussian, motion blur, JPEG compression, and salt, and pepper attacks. On the other hand, the authors of [14] proposed a method to embed a color watermark into the cover image using DCT. The proposed work employs PSO and fuzzy logic techniques to find optimal pixel values to work on. Fuzzy logic checks neighbor pixel values and find the best locations to achieve more robust and secure embedding. Results are very strong against common geometric and statistical attacks.

In [15], the Arnold Cat map, SVD, and DFT techniques were used to build a reliable watermarking approach. The cover image is applied to the DFT, then SVD is applied on the low frequencies. Similarly, a binary watermark is embedded into the selected coefficients using the Arnold Cat map algorithm. The proposed algorithm is secure, robust, and resistant against to Lossy JPEG compression attacks but the main disadvantage is the weakness against geometrical attacks, especially the cropping attack.

Authors in [16] proposed a robust watermarking algorithm for medical images using Fast Discrete Curvelet Transforms (FDCuT), DCT, and SVD transformations. FDCut is used on a medical image. which outputs three sub-bands. High-frequency coefficients are used in DCT and SVD to embed binary watermarks. In the meanwhile, the SVD method is applied to the binary watermark. Singular values in both images are exchanged. Experimental results show that the algorithm is resilient against several attacks such as Gaussian noise, resizing, filtering, noise, and cropping. Authors in [17] proposed the least significant bits algorithm for medical image watermarking. In this work, there are two types of algorithms used; special domain and frequency domain. In frequency domain watermarking, wavelet, cosine and Fourier transformations are applied to the medical cover images. A binary watermark is embedded in all techniques. Results show that the LSB embedding and extraction method in medical images gives more promising results compared to frequency domain algorithms, especially in geometric attacks. In our previous work [18], a unique watermarking method was described that leverages a hybrid Multiscale/Multiresolution frequency coefficient chosen method based on the Fast Discrete Curvelet Transform (FDCT) in combination with Singular Value Decomposition (SVD). To provide another protection layer, the Radon Transform (RT) is applied to make the method robust against various attacks. The watermark is applied to the watermarks before embedding for the sake of resilience and security.

The authors of [19] introduced a unique combination of DCT and SVD in the discrete wavelet transform (DWT) domain using least-square curve fitting based on the chaotic map. DWT is used to break down the cover picture into four sub-bands, and the low-frequency sub-band LL is partitioned into non-overlapping blocks. Then, for each block, DCT is performed while several particular middle-frequency DCT coefficients are recovered to create a modulation matrix that is used to alter the watermark. Similarly, using the canny edge detector method and the discrete cosine transform (DCT) with singular value decomposition (SVD), the authors of [20] suggested a watermarking scheme. The low-frequency coefficients and edge detection vector from the diagonal matrix of the SVD of DCT DC are combined to create a binary encrypted watermark. An edge-tracing method is used to insert watermarks. The authors of [21] presented a dual watermarking architecture for industrial picture content authentication and tamper localization. Watermarks is connected to the cover picture for tamper detection, are placed in distinct planes of the cover image.

All previous works proposed secure and robust watermarking schemes, most of them managed to overcome most common attacks, however, cropping attack is considered one of the hardest geometrical attacks especially if it is applied randomly and in multiple manner. In this work, let's propose a new watermarking scheme that is based on the Contourlet transform (CT), SVD, and Arnold transform. The proposed scheme is designed to overcome cropping attacks as the Arnold transform scrambles the watermark randomly before embedding. On the other hand, CT is preferred over other frequency domains (DWT, DCT, and DFT) as it can overcome their disadvantages such as poor directionality and failing to represent curvilinear structures. In addition, CT transform provides high directivity, reduces noise effects, and efficiently represents edges and curves [22]. Due to the increasing number of cyber-attacks and image manipulation, therefore, the proposed method bridges the gap in this topic.

3. The aim and objectives of the study

The aim of the study is to build a watermarking scheme that is perfectly resilient to geometric attacks especially cropping attack as it always shows up as a definitive challenge for most watermarking schemes if not all including state-of-the-art work.

To achieve this aim, the following objectives are accomplished:

– to build a robust watermarking method to protect image integrity;

– to make the proposed watermarking method robust against attacks especially cropping attack.

4. Object and hypothesis of the study

4. 1. Object and hypothesis of the study

In this work, a digital image watermarking scheme that resists cropping attack is proposed. Altering image information is possible when no verification techniques are conducted. This may lead to altering image information. Such protection could be achieved easily through watermarking. In this work, the contourlet transform and singular value decomposition were employed as the embedding domain, MATLAB R2015a is the implementation tool. Standard test images were employed with cropping and random cropping to test the algorithm's robustness. Multiple random attacks were applied which is has not been observed in any of the previous works in the field.

The contourlet transform, and singular value decomposition in conjunction with the Arnold cat map transformations were employed. The host image has been decomposed into the first level of contourlet transform and the highest frequency sub-bands are selected for embedding after performing the singular value decomposition on those bands where the singular value decomposition diagonal matrix is chosen to be the embedding domain. The Arnold cat map scrambles the watermark for security and resilience before inserting the binary logo. The scheme is designed to be resilient to cropping attacks alongside other geometrical and common attacks. Fig. 1 below shows the contourlet transform directional sub-band representation. Similarly, Fig. 2 shows a two-Level Contourlet Transform decomposition of Lena.

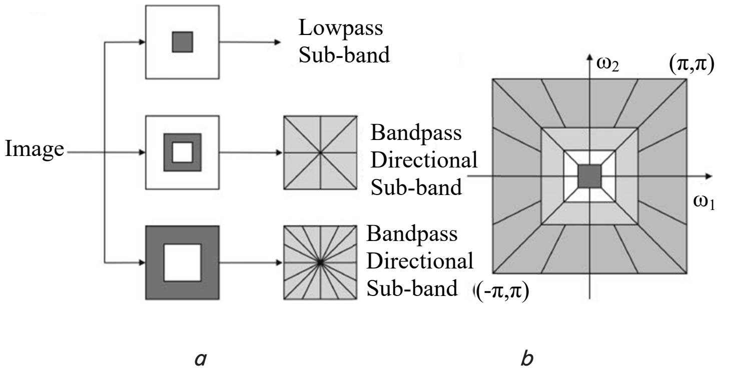

Fig. 1. Contourlet Transform directional sub-band representation: *a* – filter bank structure; *b* – idealized frequency partitioning

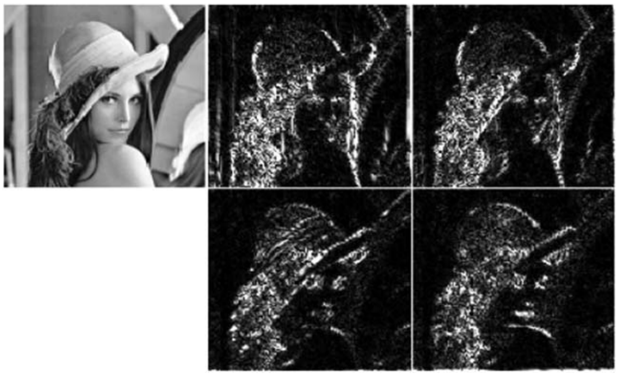

Fig. 2. Two-Level Contourlet Transform decomposition of Lena

The contourlet transform is used for its advantages over other common transforms, especially in terms of directionality.

In order to overcome the cropping attack, the proposed scheme is designed in the frequency domain specifically the Contourlet domain, which is directional and multiresolution. These properties can be combined with the singular value decomposition properties to design a robust yet imperceptible watermarking scheme.

4. 2. Arnold transformation

A scrambling algorithm is used to increase the security of the watermark to protect data from cyber-attacks and the removal of the watermark so the data will be more reliable after transformation. Due to its simplicity and periodicity, Arnold scrambling is used in image watermarking to restore the original data after several cycles, such a scrambling algorithm and the key image will be safe even if cyber extract it from watermarking. Furthermore, to increase security, relations in pixels will be broken.

Note that the cycle of Arnold transform has to be less than *N2/2* where *N* is the image size. The main idea to restore the image after several cycling by using the Arnold transform is to receive the image securely. Arnold's cat map is described in (1):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N, \qquad (1)$$

where (x, y) represents the parameters of the input image pixel and (x', y') represents the parameters of the scrambled output image pixel. Furthermore, the square image's dimensions are N. The inverse Arnold transformation can be given as in (2):

$$\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}2&-1\\-1&1\end{pmatrix}\begin{pmatrix}x'\\y'\end{pmatrix}\bmod N. \qquad (2)$$

Fig. 3 illustrates the proposed scheme embedding diagram. More details about the proposed method are illustrated in the flowchart below.

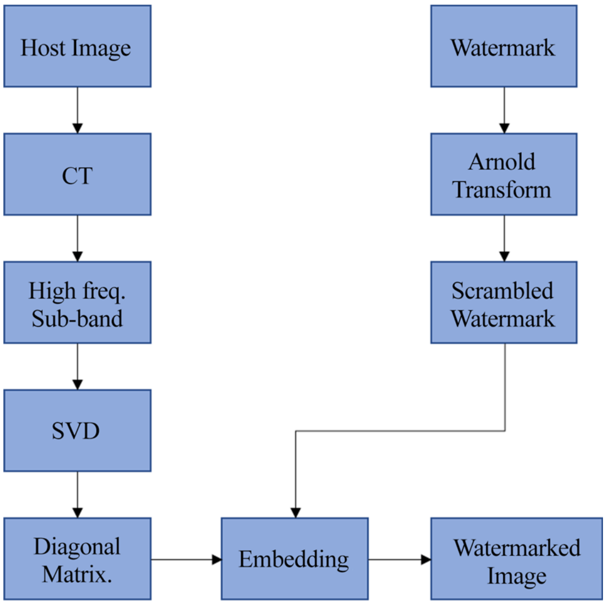

Fig. 3. Diagram of the proposed system

The host image is transformed with CT where the high-frequency sub-bad is taken. After that, SVD is applied and the watermark is inserted in the SVD diagonal matrix to generate the watermarked image.

4. 3. Embedding

The embedding algorithm is described in the pseudo code below:

```
Algorithm 1: Embedding Algorithm.
Input: $I$, $W$, $\alpha$ ($I$: host Image, $W$: binary watermark logo, $\alpha$: gain factor).
Output: $I_{Modified}$ ($I_{watermarked}$: watermarked Host):
1. Read the 128×128 binary logo watermark, which is marked with the letter $W$.
2. Transform $W$ with Arnold's transform to get the scrambled watermark denoted by $WS$.
3. Read the host medical image with a size of 1024×1024 and denote it by $I$.
4. Use the first level of decomposition of $CT$ to $I$.
5. Perform $SVD$ on the high-frequency sub-bands obtained from step 4 and select the $S$ diagonal matrix of $SVD$.
6. Insert the watermark into the $S$ diagonal matrix created in step 5:
   $S_{embed}=S+\alpha^{*}W_S$,
   where $\alpha=0.1$.
7. Apply inverse $SVD$:
   $S2_{modified}=S2+\alpha^{*}W_{RT}$.
8. Apply inverse CT to obtain the final watermarked image, which is denoted by $I_{watermarked}$.
```

4. 4. Extraction

Extraction steps are described within the following pseudo-code:

```
Algorithm 2: Extraction Algorithm.
Input: $I_{watermark}$ ($I_{modified}$: watermarked Host, $\alpha$: gain factor).
Output: $W_{extracted}$ ($W_{extracted}$: extracted watermark):
1. Use CT on $I_{watermarked}$ to get the high-frequency sub-bands.
2. Perform SVD on high-frequency sub-bands obtained from step 1 to get the watermarked image diagonal SVD matrix and denote it by $S_{watermarked}$.
3. Extract the watermark:
   $W_{extracted}=(S_{watermarked}-S)/\alpha$.
4. Apply inverse Arnold transform on $W_{extracted}$ to get the final watermark.
```

The results were assessed and compared to state-of-the-art work using peak signal-to-noise ratio and normalized correlation.

5. Research results of the proposed watermarking scheme robustness

5. 1. Imperceptibility evaluation

Fig. 4 shows the original binary payload with its scrambled version, the scrambling is carried out using the Arnold transformation with 4 iterations, the scrambling added another layer of security to the embedding mechanism which also increases the overall security of the scheme in case of watermark extraction/detection attack. In terms of perceptibility, Fig. 5 illustrates the original and watermarked test images.

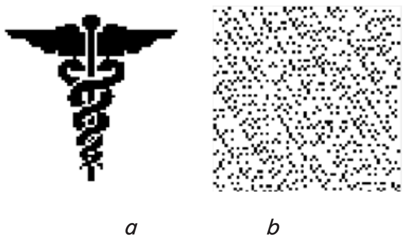

Fig. 4. Applying Scrambled watermark: *a* – original watermark; *b* – scrambled watermark

It can be noticed that the PSNR value is above 50 dB and the average PSNR value is 52.52 dB, PSNR value is the measure of how much the watermarked version is distorted, whether it is noticeably distorted or totally intact, this concludes that our scheme maintained high imperceptibility with all test images. Also, the scheme is extendable to any type of image such as medical images.

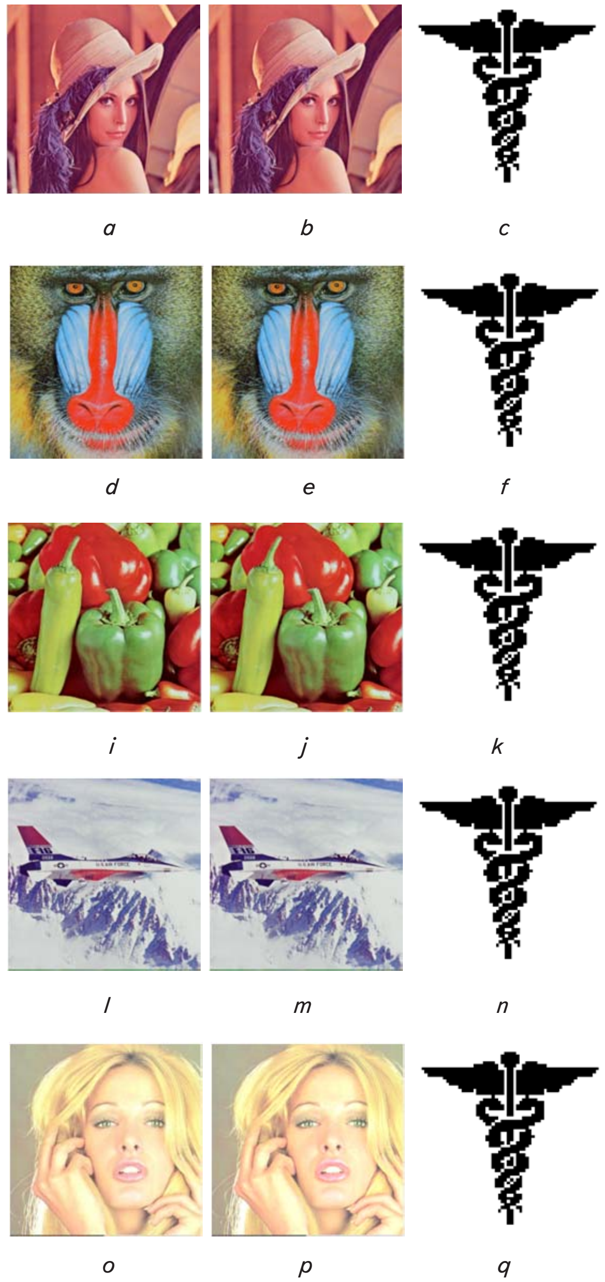

Fig. 5. Original and Watermarked test images with Peak-signal to noise ratio in dB: *a* – original test image; *b* – watermarked image (LenaPSNR=52.49); *c* – extracted watermark (NC=0.9999); *d* – original test image; *e* – watermarked image (MandrillPSNR=52.79); *f* – extracted watermark (NC=0.9999); *i* – original test image; *j* – watermarked image (PeppersPSNR=52.47); *k* – extracted watermark (NC=0.9999); *l* – original test image; *m* – watermarked image (AirplanePSNR=52.37); *n* – extracted watermark (NC=0.9999); *o* – original test image; *p* – watermarked image (GirlPSNR=52.49 dB); q – extracted watermark (NC=0.9999)

5. 2. Robustness evaluation

In terms of robustness, the scheme was sepecially designed to resist cropping attacks of any kind, thus, the main focus of this section is on testing the scheme against cropping. the scheme performed outstandingly and provided novel results as Fig. 6 shows the random cropping against the famous Lena image, random 50 % cropping, random 90 % cropping, and random multiple cropping applied on Lena image and the results were excellent as the NC value ranged from 0.8500 to NC=0.9999. Fig. 7 demonstrates the cropping attack results against which has high frequency, yet the results show high scheme robustness while NC values ranged from 0.8904 to 0.9999. The same applies to Fig. 8. The scheme maintained an NC value higher than 0.9 in almost all attack scenarios.

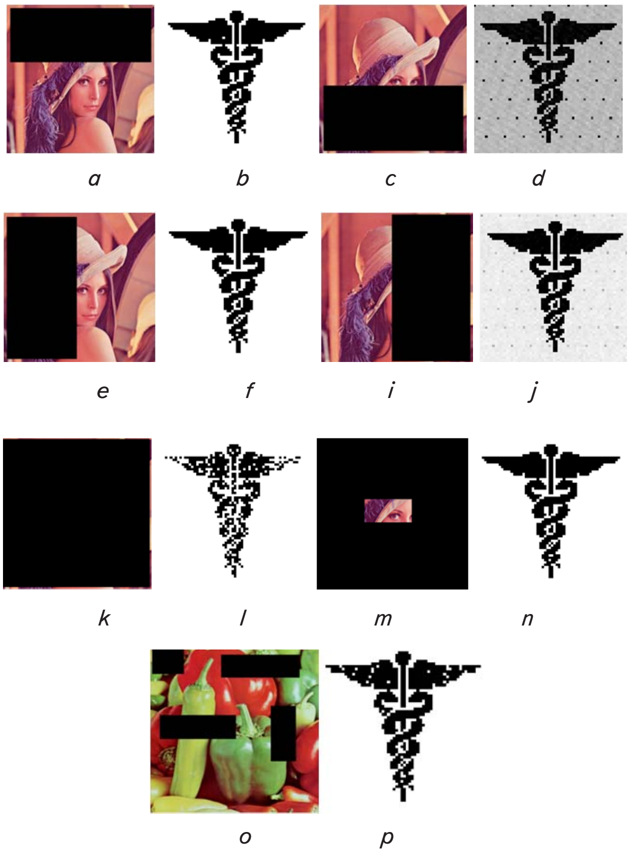

Fig. 6. Random cropping attack on lena image: *a* – attacked image (PSNR=9.28); *b* – recovered watermark (NC=0.9968); *c* – attacked image (PSNR=9.24); *d* – recovered watermark (NC=0.9622); *e* – attacked image PSNR=9.56; *f* – recovered watermark NC=0.9999; *i* – attacked image PSNR=7.48; *j* – recovered watermark (NC=0.9965); *k* – attacked image (PSNR=5.30); *l* – recovered watermark(NC=0.8500); *m* – attacked image (PSNR=5.37); *n* – recovered watermark (NC=0.9999); *o* – attacked image (PSNR=9); *p* – recovered watermark (NC=0.9992)

In Fig. 6–8, the results obtained demonstrate the novelty of our scheme as the scheme managed to resist all cropping attacks with high efficiency, as mentioned, the main goal of this work is to achieve a cropping resilient watermarking scheme, this can be proved by examining the previous results.

In order to prove the scheme's robustness, different types of attacks are applied to test the scheme's robustness against other types of attacks like common signal processing attacks. Fig. 9 illustrates the scheme's robustness against other types of attacks. The attacks were applied on all standard test images, for illustration the figure below shows the attacks on Lena image.

The results from the Fig. 6–9 prove that the scheme is resilient to cropping attack, random cropping, and multiple random cropping attacks.

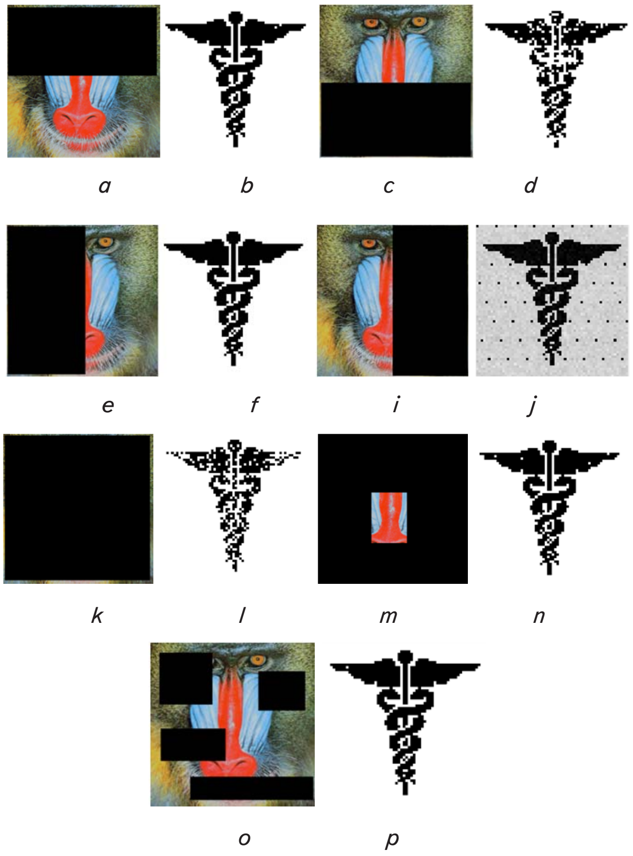

Fig. 7. Random cropping attack on Baboon image: *a* – attacked image (PSNR=9.54); *b* – recovered watermark (NC=0.9960); *c* – attacked image (PSNR=8.78); *d* – recovered watermark (NC=0.8993); *e* – attacked image (PSNR=8.72); *f* – recovered watermark (NC=0.9998)*; *i* – attacked image PSNR=8.88); *j* – recovered watermark (NC=0.8904); *k* – attacked image (PSNR=8.00); *l* – recovered watermark (NC=0.8110); *m* – attacked image (PSNR=6.34); *n* – recovered watermark (NC=0.9896); *o* – attacked image (PSNR=10.17); *p* – recovered watermark (NC=0.9991)

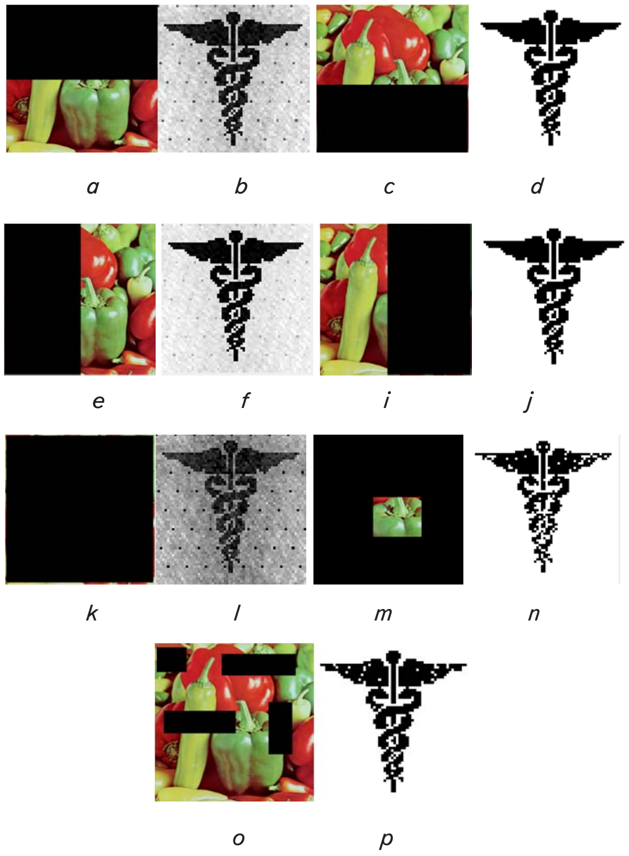

Fig. 8. Random cropping attack on Peppers image: *a* – attacked image (PSNR=8.47); *b* – recovered watermark (NC=0.9605); *c* – attacked image (PSNR=8.88); *d* – recovered watermark (NC=0. 0.9999); *e* – attacked image (PSNR=8.71); *f* – recovered watermark (NC=0.9912); *i* – attacked image (PSNR=8.64); *j* – recovered watermark (NC=0.9998); *k* – attacked image (PSNR=6.00); *l* – recovered watermark (NC=0.7906); *m* – attacked image (PSNR=6.34); *n* – recovered watermark (NC=0.9848); *o* – attacked image (PSNR=12.71); *p* – recovered watermark (NC=0.9759)

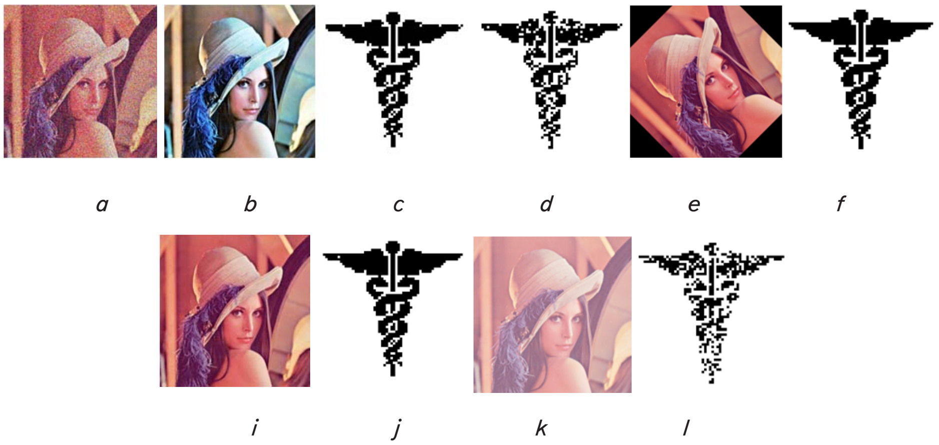

Fig. 9. Various attacks against Lena Image: *a* – attacked image (Gaussian Noise, V=0.1, PSNR=11.5); *b* – recovered watermark (NC=0.9896); *c* – attacked image(Histogram Equalization, PSNR=14.21); *d* – recovered watermark (NC=0.8969); *e* – attacked image (Rotation, PSNR=10.31); *f* – recovered watermark (NC=1); *i* – attacked image (JPEG compression, QF=25 %, PSNR=33.6); *j* – recovered watermark (NC=0.9981); *k* – attacked image (Image brightening, PSNR=13.18); *l* – recovered watermark (NC=0.7829)

Let’s compare our scheme to previous studies in the literature in Table 1, then a perceptual quality comparison is conducted (PSNR in dB). It can be seen from Table 1 that the proposed scheme outperformed other works in terms of perceptual quantity were the most relevant average PSNR value for the findings from [20] was 42.38 dB. Our proposed scheme outperformed this by an average PSNR value of 52.58 dB.

Table 1

Comparison with related work

Scheme	Image	PSNR
Proposed	Lena	52.49
	Baboon	52.79
	Peppers	52.47
[19]	Lena	40.07
	Baboon	37.14
	Peppers	42.25
[21]	Lena	42.44
	Baboon	–
	Peppers	42.33

The experiments are run on 8 GB of RAM and a 2.5 GHz Intel Core I7 processor. The simulation is conducted using a MATLAB environment, standard test images are used to determine the scheme’s robustness. Random cropping attacks were applied to prove the scheme’s resilience to cropping. Moreover, several attacks were also applied to test the scheme’s robustness in general.

6. Discussion of results of the proposed watermarking scheme efficiency

The proposed method is designed to protect image integrity and resist image attacks. The scheme performed great subjectively and objectively, the subjective assessment of the watermarked images can be examined in Fig. 5, no distortions, alteration, or editing of any kind can be noticed on the images. Moreover, subjective assessments of the extracted watermarks after every single attack again can be examined, the extracted watermarks can be recognized visually with high quality despite of the attack’s strength.

Objectively, assessments are shown in Fig. 6–8. The recovered watermark is of good quality with high NC. Fig. 9 demonstrates the proposed scheme robustness against various attacks such as image compression, noising and histogram equalization.

Table 1 illustrates that the proposed scheme has a little effect of the cover image and outperformed the related work. According to Table 1, the best PSNR reported in the work of [18, 19] is 42.25 and 42.33, respectively, for the peppers image. Our proposed scheme achieved a significant improvement for the same image by reporting a PSNR of 52.47.

The relatively high complexity in algorithm design can be considered as a disadvantageous of this work. However, this complexity can be considered as a trade-off for the achieved robustness. This point can be alleviated using artificial intelligence techniques. Hence, this study can be further developed by employing machine learning techniques to make the scheme capable of dealing with big data.

A limitation of the proposed work is represented by the number of test image used. Employing larger number of test images will be investigated in our future work.

7. Conclusions

1. With the indication of the results given it is clear that the proposed method protects image integrity while keeping good quality of the cover image. This is clear from the results and comparisons with related work where the watermarked image preserved high quality compared to other work.

2. The proposed method is robust against noising and geometric attacks especially the cropping attack. The results obtained against cropping attacks are novel in terms of robustness, as most the state-of-the-art works have not been able to tackle the multiple, random or cropping more than 80 % of the watermarked image. This was due to the scheme’s design that is based on the combination of the CT and SVD as the embedding environment, Arnold transform employment to increase the watermark security. Results obtained are novel, extracted watermarks after all types of cropping attacks are subjectively and objectively outstanding, as the NC value of the extracted watermarks ranged from 0.8 to 0.9.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed without financial support.

Data availability

Manuscript has associated data in a data repository.

References

1. The promise of telehealth for hospitals, health systems and their communities, TrendWatch (2015). American Hospital Association. Available at: https://www.aha.org/guidesreports/2015-01-20-promise-telehealth-hospitals-health-systems-and-their-communities
2. Anand, A., Singh, A. K. (2020). An improved DWT-SVD domain watermarking for medical information security. Computer Communications, 152, 72–80. doi: https://doi.org/10.1016/j.comcom.2020.01.038
3. Ananthaneni, V., Nelakuditi, U. R. (2017). Hybrid Digital Image Watermarking using Contourlet Transform (CT), DCT and SVD. International Journal of Image Processing(IJIP), 11 (3), 85–93. Available at: http://www.kresttechnology.com/krest-academic-projects/krest-major-projects/ECE/BTech%20DSP%20Major%202018/Base%20paper/8.pdf

4. Aparna, P., Kishore, P. V. V. (2019). A Blind Medical Image Watermarking for Secure E-Healthcare Application Using Crypto-Watermarking System. Journal of Intelligent Systems, 29 (1), 1558–1575. doi: https://doi.org/10.1515/jisys-2018-0370
5. Bajaj, A. (2014). Robust and reversible digital image watermarking technique based on RDWT-DCT-SVD. 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014). doi: https://doi.org/10.1109/icaetr.2014.7012955
6. Surekha, B., Swamy, G. N. (2013). Sensitive digital image watermarking for copyright protection. International Journal of Network Security, 15 (2), 95–103. Available at: https://www.researchgate.net/profile/Surekha-Borra/publication/286714951_Sensitive_Digital_Image_Watermarking_for_Copyright_Prottection/links/5709516b08ae2eb9421e2ea6/Sensitive-Digital-Image-Watermarking-for-Copyright-Prottection.pdf
7. Gavini, N. S., Borra, S. (2014). Lossless watermarking technique for copyright protection of high resolution images. 2014 IEEE REGION 10 SYMPOSIUM. doi: https://doi.org/10.1109/tenconspring.2014.6863000
8. Surekha, B., Swamy, G., Reddy, K. R. L. (2012). A novel copyright protection scheme based on Visual Secret Sharing. 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12). doi: https://doi.org/10.1109/icccnt.2012.6395968
9. Magdy, M., Ghali, N. I., Ghoniemy, S., Hosny, K. M. (2022). Multiple Zero-Watermarking of Medical Images for Internet of Medical Things. IEEE Access, 10, 38821–38831. doi: https://doi.org/10.1109/access.2022.3165813
10. Wu, P., Chen, J. (2022). A New Information Hiding Scheme Using Discrete Wavelet Transform at Physical Layer. 2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA). doi: https://doi.org/10.1109/icpeca53709.2022.9719283
11. Anand, A., Singh, A. K. (2023). Dual Watermarking for Security of COVID-19 Patient Record. IEEE Transactions on Dependable and Secure Computing, 20 (1), 859–866. doi: https://doi.org/10.1109/tdsc.2022.3144657
12. Ernawan, F., Ariatmanto, D., Musa, Z., Mustaffa, Z., Zain, J. M. (2020). An Improved Robust Watermarking Scheme using Flexible Scaling Factor. 2020 International Conference on Computational Intelligence (ICCI). doi: https://doi.org/10.1109/icci51257.2020.9247798
13. Preet, C., Aggarwal, R. K. (2017). Multiple image watermarking using LWT, DCT and arnold transformation. 2017 International Conference on Trends in Electronics and Informatics (ICEI). doi: https://doi.org/10.1109/icoei.2017.8300908
14. Gupta, N., Bhansali, A. (2021). Embedding Color Watermark by Adjusting DCT using RGB Gray Scale Watermarking. 2021 Emerging Trends in Industry 4.0 (ETI 4.0). doi: https://doi.org/10.1109/eti4.051663.2021.9619432
15. Mohammed, A. A., Abdullah, M. A. M., Elbasi, E. (2021). A Hybrid Watermarking Scheme Based on Arnold Cat Map Against Lossy JPEG Compression. 2021 International Conference on Information Security and Cryptology (ISCTURKEY). doi: https://doi.org/10.1109/iscturkey53027.2021.9654333
16. Novamizanti, L., Wahidah, I., Wardana, N. (2020). A Robust Medical Images Watermarking Using FDCuT-DCT-SVD. International Journal of Intelligent Engineering and Systems, 13 (6), 266–278. doi: https://doi.org/10.22266/ijies2020.1231.24
17. Elbasi, E., Kaya, V. (2018). Robust Medical Image Watermarking Using Frequency Domain and Least Significant Bits Algorithms. 2018 International Conference on Computing Sciences and Engineering (ICCSE). doi: https://doi.org/10.1109/iccse1.2018.8374221
18. Mohammed, A. A., Abdullah, M. A. M., Awad, S. R., Alghareb, F. S. (2022). A Novel FDCT-SVD Based Watermarking with Radon Transform for Telemedicine Applications. International Journal of Intelligent Engineering and Systems, 15 (1). doi: https://doi.org/10.22266/ijies2022.0228.07
19. Kang, X., Zhao, F., Lin, G., Chen, Y. (2017). A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. Multimedia Tools and Applications, 77 (11), 13197–13224. doi: https://doi.org/10.1007/s11042-017-4941-1
20. Mohammmed, A. A., Elbasi, E., Alsaydia, O. M. (2021). An Adaptive Robust Semi-blind Watermarking in Transform Domain Using Canny Edge Detection Technique. 2021 44th International Conference on Telecommunications and Signal Processing (TSP). doi: https://doi.org/10.1109/tsp52935.2021.9522657
21. Kamili, A., Hurrah, N. N., Parah, S. A., Bhat, G. M., Muhammad, K. (2021). DWFCAT: Dual Watermarking Framework for Industrial Image Authentication and Tamper Localization. IEEE Transactions on Industrial Informatics, 17 (7), 5108–5117. doi: https://doi.org/10.1109/tii.2020.3028612
22. Borra, S., Lakshmi, H., Dey, N., Ashour, A., Shi, F. (2017). Digital image watermarking tools: state-of-the-art. Frontiers in Artificial Intelligence and Applications, 296, 450–459.